UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/862,986	05/22/2001	Hezi Friedman	P04949 (NATI15-04949)	7516

7590 05/05/2006

William A. Munck
Novakov Davis & Munck, P.C.
13155 Noel Road, Suite 900
Dallas, TX 75240

EXAMINER	
ZAND, KAMBIZ	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 05/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/862,986
Filing Date: May 22, 2001
Appellant(s): FRIEDMAN ET AL.

William A. Munck
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 01/23/2006 appealing from the Office action mailed 08/23/2005 and 11/08/2005.

Real Party in Interest

(1) A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences, which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

A statement of the status of the claims is contained in the brief.

(4) Status of Amendments after Final

A statement identifying the status of amendments after Final is contained in the brief.

(5) Summary of Claimed Subject Matter

The summary of invention contained in the brief is correct.

(6) Grouping of Claims

A statement identifying the grouping of claims is contained in the brief.

(7) Claims Appealed

A copy of appealed claims 2, 8-10, 13, 15 and 18-20 appears on pages 2-5 and 7-8 of the appellant's Appendix A.

(8) Drawings

Copy of Formal drawings appears on the appellant's appendix B.

(9) Evidence

A statement identifying additional evidence is contained in the appellant's Appendix C.

(10) Answer to Related Proceedings

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

A statement identifying related proceedings is contained in the appellant's Appendix D.

(11) Prior Art of Record

The following is a listing of the prior art of record relied upon in the rejection of claims under appeal:

Rawlins (US 6,216,183)

Flannery (US 5,799,196)

Ben-Dor et al. (US 2002/0141418A1)

Lemay et al. (US2002/0144115A1)

(12) Grounds of Rejection to be reviewed on Appeal

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. **Claim 2** is rejected under 35 U.S.C. 103(a) as being unpatentable over Rawlins (6,216,183).

As per claim 2 Rawlins teach an apparatus for providing a secure serial bus (USB) comprising a secure channel for transferring data, wherein said apparatus comprises a secure USB domain device coupled to an external host computer, wherein said secure USB domain device comprises elements that are not accessible by said

external host computer; a USB memory device that is not accessible by said host computer;

a USB processor that is not accessible by said host computer;

a USB host controller that is not accessible by said host computer; and

an internal USB bus that couples said USB memory device, said USB processor, and said USB host controller (see fig.1 and associated text; col.3, lines 8-40,48-50; col.1, lines 21-30; col.2, lines 20-31). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize the USB memory device, processor and host controller inaccessible to the host computer so as to prevent unauthorized access to data by a malicious computer user.

2. **Claims 8-10, 13 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Flannery (5,799,196) in view of Rawlins (6,216,183).

As per claims 8 and 15 Flannery teach an apparatus and method for providing a secure universal serial bus (USB) capable of transferring information over a secure channel, said apparatus comprising: at least one host computer capable of supporting USB input/output devices, said at least one host computer comprising a USB bus, USB client software, and USB system software (see col.2, lines 5-18,12-15,18-22) but do not disclose explicitly a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing

data flows of non-confidential information. However Rawlins disclose a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information (see col.2, lines 62-67 and col.3, lines 1-18). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins's USB secure device capable of blocking of confidential data in Flannery system in order to prevent leakage of the confidential information.

As per claim 9 Flannery teach all limitation of the claim as applied above but do not explicitly disclose wherein said secure USB domain device comprises:

a plurality of USB devices;

a first set of data channels for exchanging data with each of said plurality of USB devices; and

a second set of data channels for exchanging data with said at least one host computer. However Rawlins disclose the above limitation in fig.1 and associated text. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins's USB secure device capable of blocking of confidential data in Flannery system in order to prevent leakage of the confidential information.

As per claim 10 Flannery teach an apparatus as claimed in Claim 8 wherein said secure USB domain device is embedded within said at least one host computer (see col.2, lines 12-14).

As per claim 13 Flannery disclose all limitation as applied above but do not explicitly disclose wherein said secure USB domain device is external to and coupled to said at least one host computer. However Rawlins disclose wherein said secure USB domain device is external to and coupled to said at least one host computer (see fig.1 and associated text; col.3, lines 8-18,48-50). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins's USB secure device capable of blocking of confidential data in Flannery system in order to prevent leakage of the confidential information.

3. **Claims 8-10, 13 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Flannery (5,799,196) in view of Rawlins (6,216,183) in further view of Ben-Dor et al (US2002/0141418 A1).

As per claim 20 Flannery in view of Rawlins teach all limitation of the claim as applied above but do not disclose coupling a virtual conduit interface to said secure USB domain device; coupling said virtual conduit interface to at least one non-USB device, and using said virtual conduit interface to provide a secure USB channel for transferring information to said at least one non-USB device. However Ben-Dor et al

disclose coupling a virtual conduit interface to said secure USB domain device; coupling said virtual conduit interface to at least one non-USB device, and using said virtual conduit interface to provide a secure USB channel for transferring information to said at least one non-USB device (see paragraph 73). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Ben-Dor's above limitation in Flannery in view of Rawlins in order to allow for the USB controller to interface with non-USB hardware.

4. **Claim 18** is rejected under 35 U.S.C. 103(a) as being unpatentable over Flannery (5,799,196) in view of Rawlins (6,216,183) in further view of Lemay et al (US2002/0144115 A1).

As per claim 18 Flannery teach all the limitation as applied above but do not disclose the wherein secure information is transferred between said at least one host computer and said secure USB domain device, thereby establishing at least one secure data channel between said at least one host computer and said secure USB domain device. However Rawlins disclose the wherein secure information is transferred between said at least one host computer and said secure USB domain device, thereby establishing at least one secure data channel between said at least one host computer and said secure USB domain device (see col.3, lines 49-58). Flannery in view of Rawlins however do not disclose such transferring information is in ciphered format. Lemay et al disclose this on paragraph 58 and 59. Therefore it

would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Lemay et al 's enciphering format features in Flannary in view of Rawlins to prevent the deciphering the information by an intruder.

As per claim 19 Flannery teach all limitations of the claim as applied above but do not disclose wherein data flows from a first device to a second device directly through said secure USB domain device without utilizing resources of said host computer. However Rawlins disclose wherein data flows from a first device to a second device directly through said secure USB domain device without utilizing resources of said host computer (see col.8, lines 25-32). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins utilization resources of said host computer in Flannery system in order to screen its outgoing flow and prevent access to the data from an unauthorized user.

(13) Response to Arguments

Examiner makes the following remarks with respect to Appellant's arguments in order to simplify examiner's answer:

As per independent claim 2: Appellant's arguments that Rawling does not state "no accessibility is allowed during normal operation" page 7 last paragraph of the appeal brief is not persuasive since col.3, lines 7-26 clearly disclose during the normal operation such devices not accessible since it has to monitor target endpoint address of

a USB device within the memory and such location only accessible during secure mode, therefore if such address (location) is not accessible during normal mode then how a USB device can be accessed when the address where it is found is not accessible (that is putting the address of the USB device into system memory 18 of the system 10). The problem with the appellant's arguments is that it is based on the wrong analogy, that the memory is within USB host controller 30. However the controller only transfer the target address of the USB device to the memory system 18 location. Therefore only authorized user that have access to the location of the memory may use the address of the target USB device in order to access it. Therefore the limitation "wherein said USB domain device comprises elements that are not accessible by said external host computer" is met since the domain is secure by providing only authorized access and not accessible otherwise. In support of examiner's above arguments, examiner refers to page 13 of the specification for support where a definition of secure domain creation is given and where it clearly states that two type data, one requires no intervention and the other do need intervention. In light of the page 13, fig.1 of the Rawling clearly disclose elements 32a-c as USB devices and system elements 12-30 creating the system in which the USB devices do communicate and where address for USB devices are monitored within element 18 and if secure mode is not establish the address of the USB devices not accessible and therefore Rawling teach not accessibility of the USB devices by external system during the operation.

As per independent claim 8: Rawling do disclose in col.2, lines 62-67 and col.3, lines 1-25 exactly what appellant traversing. The limitation "blocking outgoing data flows of confidential information" is met by the fact that in secure mode the access to the USB device and the flow from USB device is block unless authorized. The limitation of forwarding outgoing data flows of encrypted confidential information and forwarding outgoing data flows on non-confidential information" is met by the fact that once the authorized access to a USB device by access to the address in memory 18 is given the flow of data (confidential or non confidential, encrypted or non-encrypted) is granted in either direction.

As per claim 9, Examiner only points out the limitations "first set of data channels" and "second set of data channels" only represent communication channels (BUSES) between the devices involved regardless of lexicon used by the Appellant. Fig. 1 of Rawlings discloses existence of the communication channels, which also is also known by one of ordinary skilled in the art as buses. Col.4, lines 49-51 describe the block diagram of fig.1 comprising various buses and bus interface units.

As per claims 10 and 13, the limitation "secure USB domain device is embedded within said at least one host computer" only represent the embedding of where the address for the USB device is located, that is the memory of the computer be embedded within so by using that address one can access USB devices that externally get connected to the computer. Col.1, lines 12-14 disclose above in broadest term since the computer is set

to connect internally and externally. Furthermore such system also exists with Rawling in fig.1 in harmony with 103 rejections.

As per claim 15, Examiner points out that Applicant concede that Flannery disclose USB bus and software. Col.3, lines 7-26 clearly disclose during the normal operation such devices not accessible since it has to monitor target endpoint address of a USB device within the memory and such location only accessible during secure mode, therefore if such address (location) is not accessible during normal mode then how a USB device can be accessed when the address where it is found is not accessible (that is putting the address of the USB device into system memory 18 of the system 10). The problem with the appellant's arguments is that it is based on the wrong analogy, that the memory is within USB host controller 30. However the controller only transfer the target address of the USB device to the memory system 18 location. Therefore only authorized user that have access to the location of the memory may use the address of the target USB device in order to access it. In support of examiner's above arguments, examiner refers to page 13 of the specification for support where a definition of secure domain creation is given and where it clearly states that two type data; one requires no intervention and the other do need intervention. In light of the page 13, fig.1 of the Rawling clearly disclose elements 32a-c as USB devices and system elements 12-30 creating the system in which the USB devices do communicate and where address for USB devices are monitored within element 18 and if secure mode is not establish the

address of the USB devices not accessible and therefore Rawling teach not accessibility of the USB devices by external system during the operation.

As per claim 18 and 19 Lemay et al disclose on paragraph 58 and 59 transfer of information in enciphered format. Appellant do not dispute that fact but traverse the motivation of combining the references. However such motivation is reasonable since the enciphering/deciphering feature of Lemay adds to security of communication between USB devices and the host computer, because the secure USB device domain only protect the address for access to USB device, but when such access by authorized user is establish, then the question of secure communication is resolved by Lemay enciphering/deciphering capabilities in communication between two parties and therefore from the same environment that deals with secure access and communication, see paragraph [0040-0041] of Lemay which disclose USB environment in harmony with other references environment. Paragraph [0059] Lemay discloses the data transferred may be in encrypted (enciphered) format. Therefore it would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Lemay et al 's enciphering format features in Flannary in view of Rawlins to prevent the deciphering the information by an intruder {0059} of Lemay.

As per claim 20 Examiner makes the following remarks: USB bus driver is inherent part of USB device, or USB device would not work without it. Furthermore, in

response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e." USB bus driver",) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant traverses the motivation to combine with respect to claim 20 also not persuasive since Ben-Dor disclose tunneling between a bus and a network that is the communication channels between a BUS and other devices in the network and therefore in the same environment of network utilizing USB devices and secure domains. Paragraph [0073] of Ben-Dor disclose such harmony and environment in relation with other references combined. Motivation to combine also has support in paragraph [0074], which enables interface with other non-USB devices. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Ben-Dor's above limitation in Flannery in view of Rawlins in order to allow for the USB controller to interface with non-USB hardware.

In response to Appellant's arguments traversing motivation to combine, examiner makes the following remarks:

a) Lemay enciphering/deciphering capabilities in communication between two parties and therefore from the same environment that deals with secure access and communication, see paragraph [0040-0041] of Lemay which disclose USB environment in harmony with other references environment. Paragraph [0059]

Lemay discloses the data transferred may be in encrypted (enciphered) format. Therefore it would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Lemay et al 's enciphering format features in Flannary in view of Rawlins to prevent the deciphering the information by an intruder {0059} of Lemay.

b) Ben-Dor disclose tunneling between a bus and a network that is the communication channels between a BUS and other devices in the network and therefore in the same environment of network utilizing USB devices and secure domains. Paragraph [0073] of Ben-Dor disclose such harmony and environment in relation with other references combined. Motivation to combine also has support in paragraph [0074], which enables interface with other non-USB devices. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Ben-Dor's above limitation in Flannery in view of Rawlins in order to allow for the USB controller to interface with non-USB hardware.

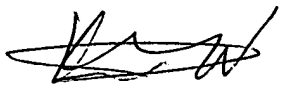
c) Rawlins disclose a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information (see col.2, lines 62-67 and col.3, lines 1-18). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins's USB secure device capable of blocking of confidential data in Flannery system in order to prevent leakage of the confidential information.

Appellant's focus on power management and not on other features of the Flannery is the problem of not recognizing the power management of Flannery do benefit other systems and methods of references used to combine, however it is the other features such as USB devices, its relationship with BUS, I/o connections that makes such motivation more proper, col.2, lines 5-18,12-15,18-22 disclose these features which corresponds to Applicant's invention environment. However it is Rawlings capabilities that add to other features of Flannery, by not only having the proper power management, which already exist in Flannery, but also adding Rawlings data blockage features in USB system of Flannery. Therefore such motivation is proper and It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins's USB secure device capable of blocking of confidential data in Flannery system in order to prevent leakage of the confidential information.

(14) Conclusion

For the above reasons, the rejection of claims 2, 8-10, 13, 15 and 18-20 should be sustained.

Respectfully submitted,



KAMBIZ ZAND
PRIMARY EXAMINER

Kambiz Zand

Primary Examiner

Art Unit 2132

April 21, 2006

Conferees

Kim Vu (SPE AU 2134)

Christopher A. Revak (Primary 2131)

5/1/06

William A. Munck

P.O. Drawer 800889

Dallas, Texas 75380.

This is in response to the appeal brief filed 01/23/2006.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Hezi Friedman *et al.*
Serial No.:	09/862,986
Filed:	May 22, 2001
For:	SECURE UNIVERSAL SERIAL BUS
Group No.:	2132
Examiner:	Kambiz Zand

APPENDIX A -
Claims Appendix

1. (Cancelled)

2. (Previously Presented) An apparatus for providing a secure serial bus (USB) comprising a secure channel for transferring data, wherein said apparatus comprises a secure USB domain device coupled to an external host computer, wherein said secure USB domain device comprises elements that are not accessible by said external host computer.

3. (Previously Presented) The apparatus as claimed in Claim 2 wherein said secure USB domain device comprises:

a USB memory device that is not accessible by said host computer;

a USB processor that is not accessible by said host computer;

a USB host controller that is not accessible by said host computer; and

an internal USB bus that couples said USB memory device, said USB processor, and said USB host controller.

4. (Previously Presented) The apparatus as claimed in Claim 3 further comprising a USB node coupled to said USB bus, said USB node capable of being coupled to a USB tree.

5. (Previously Presented) The apparatus as claimed in Claim 2 wherein said apparatus comprises a secure USB domain device embedded within a host computer.

6. (Previously Presented) The apparatus as claimed in Claim 5 wherein said secure USB domain device comprises:

a USB memory device that is not accessible by said host computer;

a USB processor that is not accessible by said host computer;

a USB host controller that is not accessible by said host computer; and

an internal USB bus that couples said USB memory device, said USB processor, and said USB host controller.

7. (Previously Presented) The apparatus as claimed in Claim 6 further comprising a virtual conduit interface coupled to said secure USB domain device and coupled to at least one non-USB device, said virtual conduit interface capable of providing a secure USB channel for transferring information to said at least one non-USB device.

8. (Previously Presented) An apparatus for providing a secure universal serial bus (USB) capable of transferring information over a secure channel, said apparatus comprising:

at least one host computer capable of supporting USB input/output devices, said at least one host computer comprising a USB bus, USB client software, and USB system software; and

a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information.

9. (Previously Presented) The apparatus as claimed in Claim 8 wherein said secure USB domain device comprises:

a plurality of USB devices;

a first set of data channels for exchanging data with each of said plurality of USB devices; and

a second set of data channels for exchanging data with said at least one host computer.

10. (Previously Presented) The apparatus as claimed in Claim 8 wherein said secure USB domain device is embedded within said at least one host computer.

11. (Previously Presented) The apparatus as claimed in Claim 10 wherein said secure USB domain device comprises:

a USB bus;

a memory coupled to said USB bus capable of storing each data packet that is at least one of sent from and received by said secure USB domain device, said memory containing a set of buffers, each of said buffers comprising data associated with at least one of: said at least one host computer and a device coupled to said at least one host computer;

circuitry coupled to said USB bus, said circuitry capable of forwarding commands and requests for information received in said secure USB domain device;

a processor coupled to said USB bus, said processor capable of at least one of: classifying data packets, controlling forwarding operations, and controlling encryption operations; and

a USB host controller coupled to said USB bus, said USB host controller capable of managing data flow between said at least one host computer and a plurality of USB devices.

12. (Previously Presented) The apparatus as claimed in Claim 11 wherein said apparatus further comprises a virtual conduit interface coupled to said secure USB domain device and coupled to at least one non-USB device, said virtual conduit interface capable of providing a secure USB channel for transferring information to said at least one non-USB device.

13. (Previously Presented) The apparatus as claimed in Claim 8 wherein said secure USB domain device is external to and coupled to said at least one host computer.

14. (Previously Presented) The apparatus as claimed in Claim 13 wherein said secure USB domain device comprises:

a USB bus;

a memory coupled to said USB bus capable of storing each data packet that is at least one of sent from and received by said secure USB domain device, said memory containing a set of buffers, each of said buffers comprising data associated with at least one of: said at least one host computer and a device coupled to said at least one host computer;

circuitry coupled to said USB bus, said circuitry capable of forwarding commands and requests for information received in said secure USB domain device;

a processor coupled to said USB bus, said processor capable of at least one of: classifying data packets, controlling forwarding operations, and controlling encryption operations; and

a USB host controller coupled to said USB bus, said USB host controller capable of managing data flow between said at least one host computer and a plurality of USB devices.

15. (Previously Presented) A method for providing a secure universal serial bus (USB) capable of transferring information over a secure channel, said method comprising the steps of:

providing at least one host computer capable of supporting USB input/output devices, said at least one host computer comprising a USB Bus, USB client software, and USB system software; and

providing a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information.

16. (Previously Presented) The method as claimed in Claim 15 wherein the step of providing a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information, comprises the steps of:

storing each data packet received by said secure USB domain device in a memory containing a set of buffers, each of said buffers comprising data associated with at least one of: said at least one host computer and a device coupled to said at least one host computer;

forwarding commands and requests for information received in said secure USB domain device;

classifying each data packet sent from said device coupled to said at least one host computer to said secure USB domain device to one of: a first data type that requires no intervention and a second data type that requires intervention according to a buffer association;

forwarding data packets of the first type that are originated at said device to said at least one host computer;

blocking data packets of the second type that contain confidential information;

forwarding data packets of the second type that contain encrypted confidential information; and

forcing any exchange of data between said at least one host computer and said device coupled to said at least one host computer to flow through said secure USB domain device.

17. (Previously Presented) The method as claimed in claim 16, wherein the step of blocking data packets of the second type that contain confidential information, and the step of forwarding data packets of the second type that contain encrypted confidential information, comprise the steps of:

interrogating a header of each data packet of the second type to reveal a type of information required;

transferring said information in an encrypted form if the information is required at another host computer for further actions; and

if said information is required for data verification:

blocking the data packet;

receiving verification information from said at least one host computer in an encrypted form;

decrypting said verification information;

comparing said decrypted verification information with information received from said device coupled to said at least one host computer; and

providing said at least one host computer with an indication verifying whether a match was detected.

18. (Previously Presented) The method as claimed in Claim 15, wherein secure information is transferred between said at least one host computer and said secure USB domain device in a enciphered form, thereby establishing at least one secure data channel between said at least one host computer and said secure USB domain device.

19. (Original) The method as claimed in Claim 15, wherein data flows from a first device to a second device directly through said secure USB domain device without utilizing resources of said host computer.

20. (Original) The method as claimed in Claim 15, further comprising the steps of:

coupling a virtual conduit interface to said secure USB domain device;

coupling said virtual conduit interface to at least one non-USB device; and

using said virtual conduit interface to provide a secure USB channel for transferring information to said at least one non-USB device.

a communication network. One or more Hosts supporting USB input/output (I/O) devices are provided. Each device comprises a Universal Serial Bus (USB), USB client software, and USB system software. A secure domain is created in which confidential outgoing data flows are either blocked or are forwarded as encrypted data, while other remaining data flows are transparently forwarded by storing each data packet sent from, or received by, the secure domain in a memory that contains a set of buffers. Each of the buffers comprises data that is associated with the Host or with the device. Commands and/or requests for information received in the secure domain are transparently forwarded to the corresponding devices. Each data packet sent from the devices to the secure domain is classified to a first data type that requires no intervention, or to a second data type that requires intervention according to the buffer association. Data packets of the first type that are originated at the devices are transparently forwarded to the Host. Data packets of the second type are blocked, or forwarded in an encrypted form. Any exchange of data between the Host and a device is forced to flow through the secure domain.

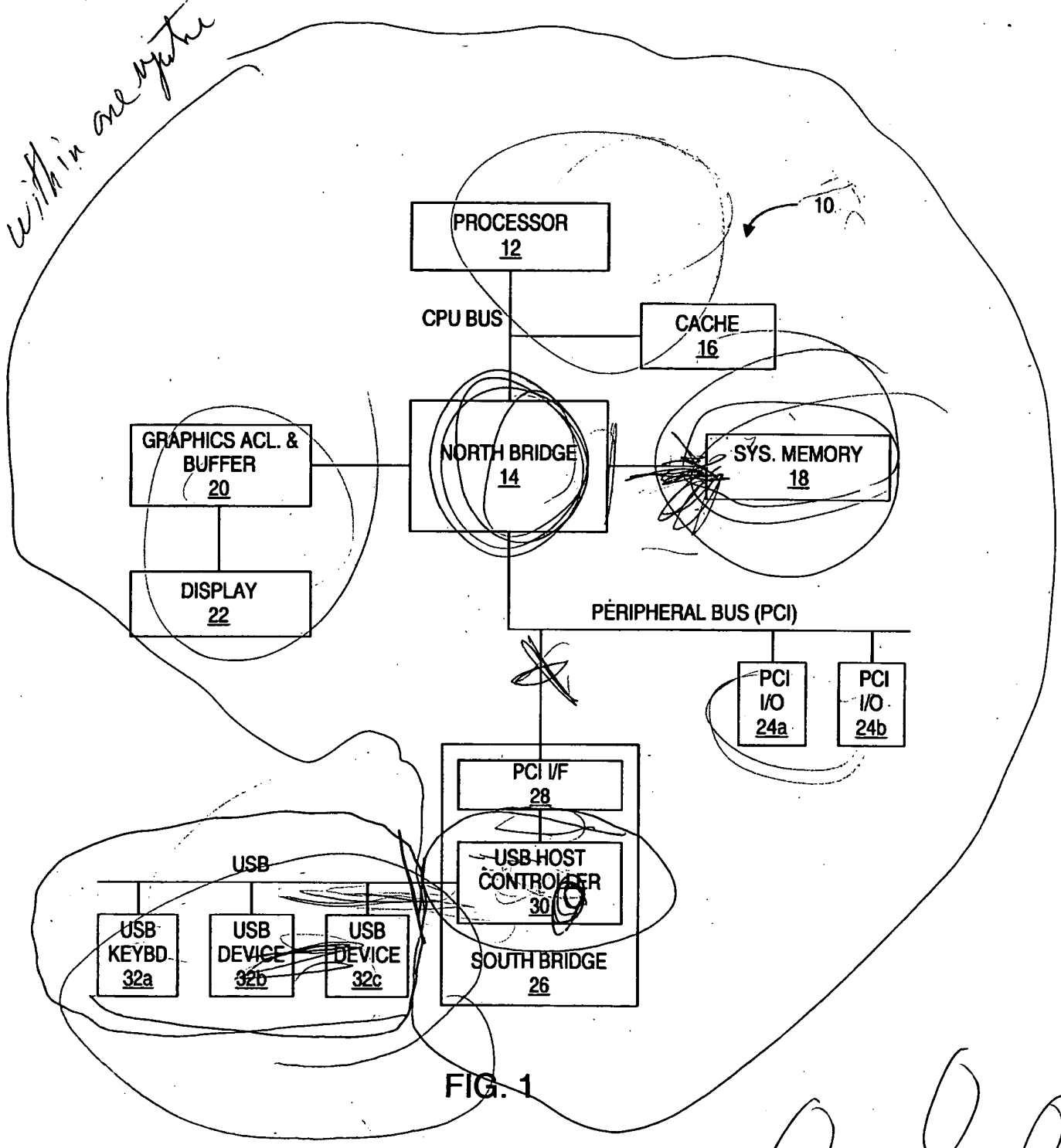
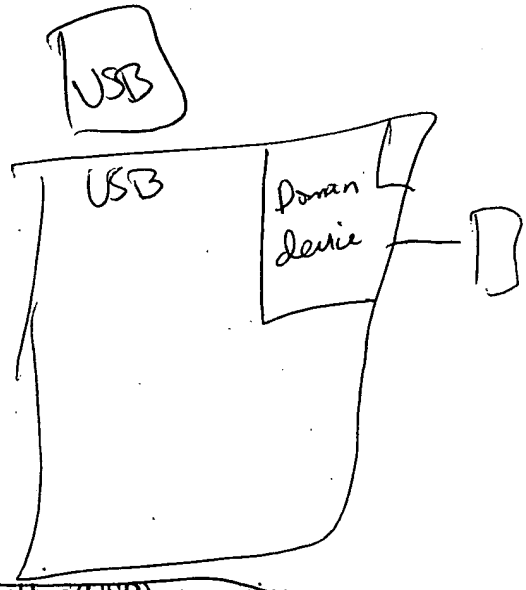

10
PROCESSOR
12
CPU BUS
CACHE
16
GRAPHICS ACL. & BUFFER
20
NORTH BRIDGE
14
SYS. MEMORY
18
DISPLAY
22
PERIPHERAL BUS (PCI)
PCI I/O
24a
PCI I/O
24b
PCI I/F
28
USB
USB HOST CONTROLLER
30
USB KEYBD
32a
USB DEVICE
32b
USB DEVICE
32c
SOUTH BRIDGE
26

FIG. 1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

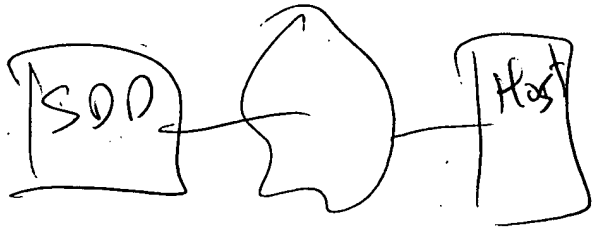
In re application of:	Hezi Friedman *et al.*
Serial No.:	09/862,986
Filed:	May 22, 2001
For:	SECURE UNIVERSAL SERIAL BUS
Group No.:	2132
Examiner:	Kambiz Zand



APPENDIX A - Claims Appendix

1. (Cancelled)

2. (Previously Presented) An apparatus for providing a secure serial bus (USB) comprising a secure channel for transferring data, wherein said apparatus comprises a secure USB domain device coupled to an external host computer, wherein said secure USB domain device comprises elements that are not accessible by said external host computer.



Office Action Summary	Application No.	Applicant(s)	
	09/862,986	FRIEDMAN ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-5, 7-10, 13, 15 and 18-20* is/are rejected.

7)☒ Claim(s) *6,7,11,12,14,16 and 17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 March 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Kambiz Zand

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claim 1 has been cancelled.
4. Claims 2, 5, 8, 9, 11 and 13-18 have been amended.
5. Claims 1-20 are pending.
6. Examiner approves the amendments to the specification by the applicant.

Response to Arguments

7. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

- In response to applicant's arguments that Rawlins teach accessibility of USB device with host computer in contrast with applicant's invention where no such accessibility allowed, examiner makes the following remarks: there is no accessibility between the host and the USB device unless authorized, and no accessibility is allowed during normal operation. Claim 11 of the applicant does show accessibility between USB devices and the host computer in contrast with applicant's arguments. Examiner however suggests if there is an element that is specifically not accessible by the host computer or external computer

whatsoever, then such element should be clearly presented in the claim language. Examiner would reconsider if such clarity be presented only if such clarity does not raise new issue that necessitate further consideration or search.

- Applicant's arguments with respect to claims 6, 7, 11, 12, 14, 16, 17 are persuasive.

Claim Objections

8. **Claims 3-7 and 10-14** are objected to because of the following informalities: typo error. Examiner suggests the following corrections:

Claim 3-7 and 10-14:

- Replacement of the phrase "A" (line 1, first occurrence) with the phrase "the".

Claim Rejections - 35 USC § 103

9. **Claims 2 and 3** are rejected under 35 U.S.C. 103(a) as being unpatentable over Rawlins (6,216,183).

As per claims 2 and 3 Rawlins teach an apparatus for providing a secure serial bus (USB) comprising a secure channel for transferring data, wherein said apparatus comprises a secure USB domain device coupled to an external host computer, wherein said secure USB domain device comprises elements that are not accessible

by said external host computer; a USB memory device that is not accessible by said host computer;

a USB processor that is not accessible by said host computer;

a USB host controller that is not accessible by said host computer; and

an internal USB bus that couples said USB memory device, said USB processor, and said USB host controller (see fig.1 and associated text; col.3, lines 8-40,48-50; col.1, lines 21-30; col.2, lines 20-31). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize the USB memory device, processor and host controller inaccessible to the host computer so as to prevent unauthorized access to data by a malicious computer user.

As per claim 4 Rawlins teach an apparatus as claimed in Claim 3 further comprising a USB node coupled to said USB bus, said USB node capable of being coupled to a USB tree (see fig.1 and associated text).

10. **Claim 5** is rejected under 35 U.S.C. 103(a) as being unpatentable over Rawlins (6,216,183) in view of Flannery (5,799,196).

As per claim 5 Rawlins teach all limitations of the claim as applied above but do not disclose wherein said apparatus comprises a secure USB domain device embedded within a host computer. However Flanny disclose the above limitation on col.2, lines 12-14 and 18-22. It would have been obvious to one of ordinary skilled in the art at

the time the invention was made to utilize embedded USB device in Rawlins in order to create hierarchical topology that enhances the scalability of the computer system in order to connect more devices to the root of the host for efficiency reasons.

11. **Claims 8-10, 13 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Flannery (5,799,196) in view of Rawlins (6,216,183).

As per claims 8 and 15 Flannery teach an apparatus and method for providing a secure universal serial
bus (USB) capable of transferring information over a secure channel, said apparatus comprising: at least one host computer capable of supporting USB input/output devices, said at least one host computer comprising a USB bus, USB client software, and USB system software (see col.2, lines 5-18,12-15,18-22) but do not disclose explicitly a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information. However Rawlins disclose a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information (see col.2, lines 62-67 and col.3, lines 1-18). It would have been obvious to one of ordinary skilled in the art at the

time the invention was made to utilize Rawlins's USB secure device capable of blocking of confidential data in Flannery system in order to prevent leakage of the confidential information.

As per claim 9 Flannery teach all limitation of the claim as applied above but do not explicitly disclose wherein said secure USB domain device comprises:
a plurality of USB devices;
a first set of data channels for exchanging data with each of said plurality of USB devices; and
a second set of data channels for exchanging data with said at least one host computer. However Rawlins disclose the above limitation in fig.1 and associated text. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins's USB secure device capable of blocking of confidential data in Flannery system in order to prevent leakage of the confidential information.

As per claim 10 Flannery teach an apparatus as claimed in Claim 8 wherein said secure USB domain device is embedded within said at least one host computer (see col.2, lines 12-14).

As per claim 13 Flannery disclose all limitation as applied above but do not explicitly disclose wherein said secure USB domain device is external to and

coupled to said at least one host computer. However Rawlins disclose wherein said secure USB domain device is external to and coupled to said at least one host computer (see fig.1 and associated text; col.3, lines 8-18,48-50). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins's USB secure device capable of blocking of confidential data in Flannery system in order to prevent leakage of the confidential information.

12. **Claims 8-10, 13 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Flannery (5,799,196) in view of Rawlins (6,216,183) in further view of Ben-Dor et al (US2002/0141418 A1).

As per claim 20 Flannery in view of Rawlins teach all limitation of the claim as applied above but do not disclose coupling a virtual conduit interface to said secure USB domain device; coupling said virtual conduit interface to at least one non-USB device, and using said virtual conduit interface to provide a secure USB channel for transferring information to said at least one non-USB device. However Ben-Dor et al disclose coupling a virtual conduit interface to said secure USB domain device; coupling said virtual conduit interface to at least one non-USB device, and using said virtual conduit interface to provide a secure USB channel for transferring information to said at least one non-USB device (see paragraph 73). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Ben-Dor's above limitation in Flannery in view of Rawlins in order to allow for the USB controller to interface with non-USB hardware.

13. **Claim 18** is rejected under 35 U.S.C. 103(a) as being unpatentable over Flannery (5,799,196) in view of Rawlins (6,216,183) in further view of Lemay et al (US2002/0144115 A1).

As per claim 18 Flannery teach all the limitation as applied above but do not disclose the wherein secure information is transferred between said at least one host computer and said secure USB domain device, thereby establishing at least one secure data channel between said at least one host computer and said secure USB domain device. However Rawlins disclose the wherein secure information is transferred between said at least one host computer and said secure USB domain device, thereby establishing at least one secure data channel between said at least one host computer and said secure USB domain device (see col.3, lines 49-58). Flannery in view of Rawlins however do not disclose such transferring information is in ciphered format. Lemay et al disclose this on paragraph 58 and 59. Therefore it would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Lemay et al 's enciphering format features in Flannary in view of Rawlins to prevent the deciphering the information by an intruder.

As per claim 19 Flannery teach all limitations of the claim as applied above but do not disclose wherein data flows from a first device to a second device directly through said secure USB domain device without utilizing resources of said host

computer. However Rawlins disclose wherein data flows from a first device to a second device directly through said secure USB domain device without utilizing resources of said host computer (see col.8, lines 25-32). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins utilization resources of said host computer in Flannery system in order to screen its outgoing flow and prevent access to the data from an unauthorized user.

Allowable Subject Matter

14. **Claims 6, 7, 11, 12, 14, 16 and 17** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

08/19/2005

AU2132